© Vasiliu Ye. Stacks of quantum cryptography protocols // Ukrainian Scientific Journal of Information Security, 2014, vol. 20, issue 1, p. 48-54.

СТЕКИ ПРОТОКОЛІВ КВАНТОВОЇ КРИПТОГРАФІЇ

Євген Васіліу

Одеська національна академія зв'язку ім. О.С. Попова, Україна

ВАСІЛІУ Євген Вікторович, д.т.н.

Рік і місце народження: 1966, Ялта, Крим, Україна.
Освіта: Одеський державний університет імені І.І. Мечникова, 1990.
Посада: директор Навчально-наукового інституту «Радіо, телебачення та інформаційної безпеки» з 2013 року.
Наукові інтереси: квантова криптографія, квантові протоколи розподілення ключів, квантові протоколи прямого безпечного зв'язку, квантові протоколи розділення секрету, квантова стеганографія.
Публікації: понад 100 наукових публікацій, серед яких 4 монографії, понад 60 наукових статтей, матеріали конференцій, патенти.
E-mail: vasiliu@ua.fm

***Анотація**. У статті детально проаналізовано стек протоколів квантового розподілення ключів, який ґрунтується на протоколі з передаванням одиночних кубітів – протоколі BB84. На підґрунті цього аналізу розроблено повний стек протоколів квантового прямого безпечного зв'язку на основі пінг-понг протоколів. Розроблений стек містить в собі такі основні протоколи: підсилення секретності, завадостійке кодування, квантове передавання інформації. При цьому розроблений стек протоколів квантового безпечного зв'язку придатний при використанні будь-якого варіанту пінг-понг протоколу в якості базового. Розглянуто основні відмінності між стеками протоколів квантового розподілення ключів та квантового прямого безпечного зв'язку, які обумовлені різним призначення цих протоколів, різними типами передаваної інформації та відповідно різними вимогами до їх безпеки.*

***Ключові слова**: квантова криптографія, кубіт, квантові протоколи розподілення ключів, квантові протоколи прямого безпечного зв'язку, стеки протоколів.*

Вступ. Характерною рисою сучасної високотехнологічної цивілізації є інформатизація, яка полягає у впровадженні новітніх інформаційних технологій в усі сфери діяльності суспільства. При цьому постійно збільшується кількість важливої інформації, яка обробляється та передається в інформаційно-комунікаційних системах, а її передавання все частіше здійснюється за допомогою відкритих комп'ютерних систем зв'язку, таких як Інтернет. Зважаючи на постійно наростаючу кількість кібератак на інформаційні ресурси по всьому світу, спрямованих на порушення конфіденційності, цілісності, достовірності та доступності інформації, розроблення та впровадження нових ефективних систем захисту інформації, зокрема систем для забезпечення безпечного обміну даними через відкриті мережі, є нагальною необхідністю.

Одним з найважливіших напрямів забезпечення конфіденційності інформації є її захист криптографічними методами. В останні два десятиріччя з'явився та швидко розвивається новий підхід до криптографічного захисту інформації, що отримав назву квантової криптографії [1–4]. На сьогодні квантова криптографія містить в собі методи захисту конфіденційної інформації, які мають відповідні аналоги і в класичній криптографії, а саме: квантове розподілення секретних ключів для їх подальшого використання в симетричних криптосистемах, квантовий прямий безпечний зв'язок (передавання секретних повідомлень без шифрування), квантове розділення секрету, квантовий потоковий шифр, квантовий цифровий підпис тощо [4]. Використання специфічних властивостей квантових систем, які служать носіями інформації в протоколах квантової криптографії, дає можливість досягти при вирішенні деяких завдань захисту інформації безумовної (теоретико-інформаційної) стійкості, яка не залежить від обчислювальних та інших можливостей зловмисника. Це є основною перевагою квантових криптографічних методів над традиційними, зокрема над методами асиметричної криптографії, які мають тільки обчислювальну стійкість.

Одним з найбільш розвинених на сьогодні напрямів квантової криптографії є квантове розподілення ключів, ця технологія вже реалізована декількома компаніями у вигляді готових пристроїв [5, 6]. Інший напрям – квантовий прямий безпечний зв'язок – поки що існує тільки у вигляді теоретичних схем та поодиноких експериментів, але на даний час розроблено велику кількість відповідних протоколів та досліджена їх стійкість до різноманітних атак [4, 7–14]. У протоколах квантового прямого безпечного зв'язку легітимні користувачі взагалі не використовують шифрування, а передають секретну інформацію напряму, тобто кодують безпосередньо відкритий текст повідомлення квантовими станами

фотонів. Легітимні користувачі обмінюються фотонами квантовим каналом зв'язку і виконують певні унітарні операції і вимірювання над ними, а також обмінюються додатковою інформацією звичайним (не квантовим) відкритим каналом з автентифікацією. На практиці як квантові канали використовують оптоволоконні лінії зв'язку, або оптичні бездротові канали.

Але як квантове розподілення ключів, так і квантовий прямий безпечний зв'язок не можуть обмежитись тільки передаванням квантових станів. Для забезпечення теоретико-інформаційного рівня стійкості потрібні додаткові процедури, які повинні бути включені у відповідні стеки протоколів квантового розподілення ключів та прямого зв'язку. На даний час стек проколів квантового розподілення ключів в цілому розроблений [1]. Для квантових протоколів безпечного зв'язку на теперішній час розроблені тільки окремі процедури [14].

Метою цієї роботи є розробка повного стеку протоколів квантового прямого безпечного зв'язку для випадку, коли в якості базового використовується пінг-понг протокол, на підґрунті аналізу стеку протоколів квантового розподілення ключів.

Стек протоколів квантового розподілення ключів. Проаналізуємо стек протоколів квантового розподілення ключів на базі протоколу з передаванням одиночних фотонів – BB84 [1–3]. Нехай одна зі сторін протоколу – суб'єкт *A* генерує та передає другій стороні – суб'єкту *B* повністю випадкову бітову строку, з якої потім буде сформований випадковий секретний ключ. У протоколі BB84 біти кодуються поляризаційними квантовими станами фотонів в двох базисах: вертикально-горизонтальному та діагональному. Суб'єкт *A* випадковим чином вибирає базис і поляризацію своїх однофотонних імпульсів і посилає їх суб'єктові *B*, тобто суб'єкт *A* з однаковою ймовірністю посилає один із чотирьох квантових станів:

$$|0\rangle,\ |1\rangle,\ |\bar{0}\rangle=\frac{1}{\sqrt{2}}\left(|0\rangle+|1\rangle\right),\ |\bar{1}\rangle=\frac{1}{\sqrt{2}}\left(|0\rangle-|1\rangle\right). \quad (1)$$

Випадкова поляризація фотонів вибирається тому, що ключ повинен бути випадковою послідовністю бітів, а два базиси потрібні для того, щоб перешкодити зловмиснику (суб'єктові *E*) правильно реєструвати поляризацію фотонів.

Для кожного фотона суб'єкт *B* випадковим чином вибирає базис і вимірює поляризацію у вибраному базисі. У результаті такої квантової передачі суб'єкт *B* отримає послідовність бітів тієї ж довжини (в ідеальному квантовому каналі), що відправив суб'єкт *A*, яку називають сирим ключем. Зрозуміло, що внаслідок загасання в реальному квантовому каналі та недосконалості реєструвальних датчиків, частина однофотонних імпульсів не буде зареєстрована суб'єктом *B*, і довжина отриманої ним строки бітів буде менша за ту, що передавав суб'єкт *A*.

Таким чином, передавання одиночних фотонів в двох взаємно незміщених базисах при випадковому виборі як поляризації у конкретному базисі, так і самих базисів, є першим елементом стеку квантового протоколу розподілення ключа, який базується на передаванні одиночних квантових станів.

Наступним елементом стеку є процедура просіювання ключа, яка виконується з використанням звичайного (не квантового) відкритого каналу зв'язку, але обов'язково зі взаємною автентифікацією суб'єктів *A* і *B*, і складається з наступних дій [1-3].

Суб'єкт *B* повідомляє суб'єктові *A* відкритим каналом, який базис він використав для кожного вимірювання, при цьому, зрозуміло, не повідомляючи результати самих вимірювань. Суб'єкт *A* повідомляє, які базиси використовував він для кодування бітів. Далі суб'єкти *A* і *B* відкидають всі біти, що відповідають випадкам, коли вони використали різні базиси, а також всі біти суб'єкта *A*, коли апаратура суб'єкта *B* взагалі не зареєструвала фотон. У результаті легітимні користувачі одержують так званий просіяний ключ, однакової довжини. Так як в протоколі BB84 суб'єкт *B* вгадує базис, використаний суб'єктом *A*, в середньому в половині випадків, то довжина просіяного ключа буде близько половини від довжини сирого ключа. При наявності загасання в квантовому каналі, зрозуміло, що довжина просіяного ключа ще зменшується, у відсотковому відношенні на величину порядку середнього рівня загасання в каналі.

Наступний – третій елемент стеку квантових протоколів розподілення ключів – протокол виявлення атаки пасивного перехоплення. Оскільки для кодування інформації поляризаційними станами суб'єкт *A* використовує один з двох базисів випадковим чином, то для атакуючого немає способу визначити, у якому базисі проводити вимірювання. Він може тільки також випадково вибрати базис, виконати вимірювання стану фотона в цьому базисі та відправити суб'єктові *B* новий фотон у тому ж стані, що він отримав у результаті вимірювання. Це приводить до помилок у бітовому рядку, який одержує суб'єкт *B*. Описані дії суб'єкта *B* називаються атакою "перехоплення – повторної посилки кубітів" [1–3]. Існують й більш складні атаки, коли зловмисник використовує допоміжні квантові системи (проби), які переплутує з фотонами, що передаються суб'єктом *A*. Потім зловмисник зберігає ці проби у себе в квантової пам'яті до того моменту, коли суб'єкт *B* оголошує базиси, і виконує вимірювання станів проб [3, 15]. Такі атаки також призводять до помилок у бітовому рядку суб'єкта *B*, оскільки операції переплутування змінюють стани передаваних фотонів, але при деякої заданої кількості помилок, що створюються атакою зловмисника, він зможе одержати більше інформації, ніж при атаці "перехоплення – повторної посилки кубітів" [15].

Таким чином, на третьому етапі протоколу легітимні користувачі повинні оцінити рівень помилок, що виникли на першому етапі – при квантовому передаванні. Для цього вони вибирають деяку підмножину бітів із просіяного ключа й порівнюють їх, користуючись відкритим каналом зв'язку. Якщо рівень помилок не перевищує деякого заданого, наприклад, 11%, якщо у зловмисника є можливість провести когерентну атаку, або 14,6%, якщо він може проводити тільки некогерентні атаки, то легітимні користувачі можуть продовжувати протокол встановлення ключа [2, 15]. Зрозуміло, що виявлені помилки можуть бути обумовлені не тільки атакою, а і

природними завадами при квантовому передаванні, й не існує способу розрізнити ці дві причини помилок. Тому при прийнятті рішення про продовження або припинення протоколу встановлення ключа легітимні користувачі повинні врахувати й природний рівень завад в даному квантовому каналі (якій повинен бути відомий заздалегідь).

Якщо рівень помилок при квантовому передаванні не перевищував допустимий, то легітимні користувачі відкидають біти, які були вибрані для оцінки рівня помилок (оскільки вони можуть стати відомими зловмиснику), та виконують наступний четвертий елемент стеку квантового розподілення ключів – протокол виправлення помилок в бітових строках, що вони мають на даний момент. Якщо ж рівень помилок перевищує допустимий, то протокол необхідно перервати і виконати знову спочатку (з використанням іншого каналу для квантового передавання на першому етапі стеку протоколів).

Для виправлення помилок в бітових строках, що одержані легітимними користувачами з просіяного ключа після оцінки рівня помилок, на даний час розроблено низку протоколів [3, 16–18]. Найчастіше при практичній реалізації протоколу BB84 використовують каскадний протокол виправлення помилок [3, 15]. Легітимні користувачі ділять одержані строки на блоки фіксованої довжини. Для кожного блоку обидві сторони перевіряють, чи містить він непарне число помилок відповідно до парності блоку. Якщо в блоці є непарне число помилок, то обидві сторони знаходять і виправлять помилку за допомогою алгоритму двійкового пошуку. Процес може виконуватись у декілька раундів. Якщо немає ніяких помилок в l послідовних раундах, то бітові строки легітимних користувачів співпадають з ймовірністю $1 - 2^{l}$ [16].

Останній – п'ятий елемент стеку квантового розподілення ключів – протокол підсилення секретності. Після виконання протоколу виправлення помилок у легітимних користувачів з високою імовірністю є ідентичні узгоджені бітові строки – узгоджений ключ. Вони також точно знають рівень помилок, що був оцінений в протоколі виявлення помилок. Легітимні користувачі постулюють, що всі помилки були обумовлені атакою пасивного перехвату. Крім того, вони враховують витік інформації під час виконання протоколу виправлення помилок, якщо він міг бути. Звідси вони виводять t – число бітів, на яке повинний бути скорочений узгоджений ключ, щоб зменшити інформацію зловмисника про фінальний ключ нижче заданого, як завгодно малого значення. Далі для даного t передавальна сторона генерує випадкову двійкову матрицю розміром $(n - t) \times n$, де n – довжина узгодженого ключа, і відкрито, тобто без за шифрування, передає її приймальній стороні. Тоді обидва легітимних користувачі обчислюють фінальний секретний ключ (довжиною $n - t$) множенням за модулем 2 цієї матриці на узгоджений ключ.

На рис.1 показано стек протоколів квантового розподілення ключів з використанням протоколу BB84 у якості базового. Відзначимо, що на даний час запропоновано велику кількість протоколів квантового розподілення ключів, що ґрунтуються як на передаванні одиночних квантових систем розмірності більше за два, так і на використанні властивості переплутаності (зчепленості) квантових систем, що складаються з двох та більшої кількості фотонів [1, 2, 4]. Показаний на рис.1 стек протоколів, з деякими відмінностями, що стосуються в основному квантового передавання, процедур виявлення атак та виправлення помилок, придатний і у випадку використання в якості базового одного з цих удосконалених протоколів.

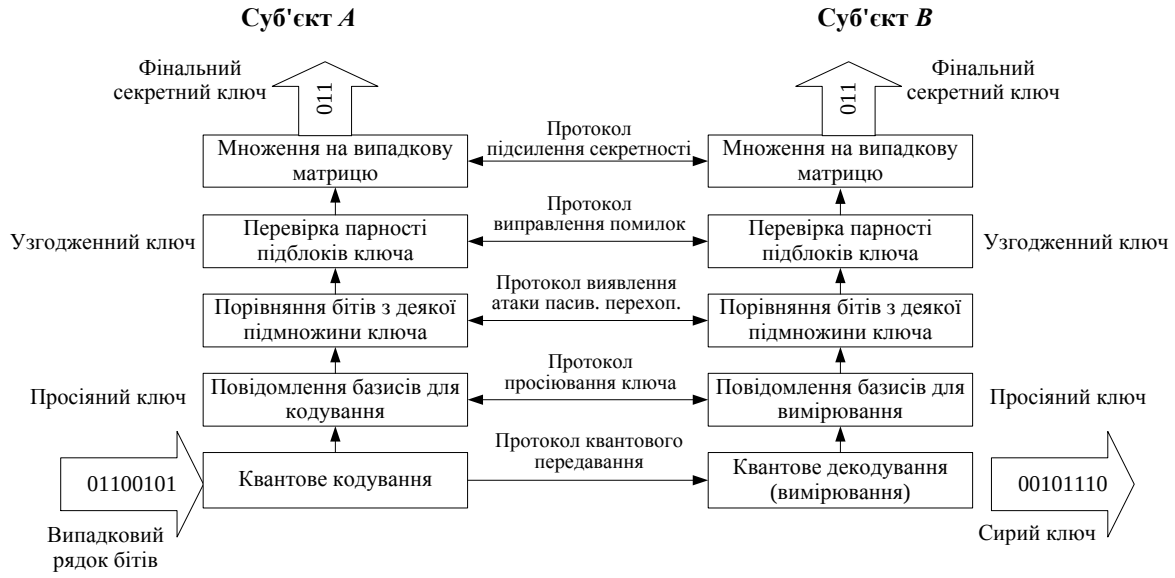

Рис.1. Стек протоколів квантового розподілення ключів

Стек протоколів квантового прямого безпечного зв'язку. Розробимо тепер повний стек протоколів квантового прямого безпечного зв'язку. В якості базового будемо використовувати пінг-понг протокол з парами повністю переплутаних кубітів та квантовим надщільним кодуванням [13].

Між протоколами квантового розподілення ключів та квантового прямого безпечного зв'язку є принципова різниця. В протоколах розподілення ключів передана за допомогою ортогональних

квантових станів інформація не є цінною для зловмисника, що виконує підслуховування, до тих пір, поки легітимні користувачі не узгодили фінальний ключ, тобто не домовились, що одержані ними після підсилення секретності однакові бітові строки вони будуть використовувати, як секретний ключ. Тому допускається деякий витік інформації при квантовому розподіленні ключів. Головна вимога полягає в тому, щоб цей витік не перевищував деякої заданої величини, яка пов'язана з граничним рівнем помилок у легітимних користувачів, як це описано в попередньому розділі статті. Якщо ж витік інформації при квантовому передаванні виявився неприпустимим, то легітимні користувачі переривають протокол і починають вісь стек протоколів квантового розподілення ключів спочатку. При цьому інформація, вже перехоплена зловмисником, не буде мати для нього ніякої цінності.

При використанні для передавання інформації протоколів квантового прямого безпечного зв'язку ситуація є принципово відмінною. Ці протоколи призначені для прямого, тобто без використання шифрування, передавання конфіденційної інформації. Тому для агента, що виконує атаку пасивного перехоплення, цінним є кожен перехоплений біт. Звідси випливає, що вимоги до безпечності протоколів квантового прямого безпечного зв'язку є значно вищими, ніж до безпечності квантових протоколів розподілення ключів.

Протоколи прямого безпечного зв'язку можна поділити на два класи в залежності від того, якій рівень стійкості вони гарантують самі по собі (тобто без додаткових процедур підсилення стійкості) [4]. Перший клас – протоколи з передаванням квантових систем великими блоками, які складають більшість запропонованих на сьогодні квантових протоколів безпечного зв'язку. Другий клас – протоколи з використанням окремих переплутаних квантових станів на кожному раунді протоколу.

Перший клас протоколів дозволяє виявити прослуховування квантового каналу до початку передачі самого повідомлення й таким способом гарантувати безпеку передачі – якщо прослуховування виявлене до передачі повідомлення, то легітимні сторони переривають сеанс і ніяка інформація не попадає до зловмисника. Таким чином, клас протоколів з передаванням квантових систем блоками забезпечує теоретико-інформаційний рівень стійкості. Але для зберігання великих блоків квантових систем потрібна квантова пам'ять великого об'єму. Технологія квантової пам'яті активно розробляється на даний час, але вона поки ще далека від масового застосування в стандартному встаткуванні. Тому, з погляду технічної реалізації, перевагу мають протоколи другого класу, у яких передача здійснюється невеликими групами квантових систем за один цикл протоколу. Таких протоколів запропоновано небагато, і найбільш відомим та простим з них є пінг-понг протокол та його різні варіанти. Саме цей протокол оберемо для побудови стеку протоколів квантового прямого безпечного зв'язку.

Розглянемо коротко схему пінг-понг протоколу з парами повністю переплутаних кубітів та квантовим надщільним кодуванням [11, 13]. Існують чотири повністю переплутаних ортогональних стани пари кубітів (стани Белла):

$$\left|\phi^+\right\rangle = \left(\left|0\right\rangle\left|0\right\rangle + \left|1\right\rangle\left|1\right\rangle\right)/\sqrt{2}\,,\quad \left|\phi^-\right\rangle = \left(\left|0\right\rangle\left|0\right\rangle - \left|1\right\rangle\left|1\right\rangle\right)/\sqrt{2}\,,$$
$$\left|\psi^+\right\rangle = \left(\left|0\right\rangle\left|1\right\rangle + \left|1\right\rangle\left|0\right\rangle\right)/\sqrt{2}\,,\quad \left|\psi^-\right\rangle = \left(\left|0\right\rangle\left|1\right\rangle - \left|1\right\rangle\left|0\right\rangle\right)/\sqrt{2}\,, \quad (2)$$

де стани $\left|0\right\rangle$ і $\left|1\right\rangle$ відповідають горизонтальній і вертикальній поляризації фотонів.

Суб'єкт *B* (одержувач) приготовляє пару фотонів у стані $\left|\psi^+\right\rangle$. Він зберігає один фотон у себе й посилає суб'єктові *A* (відправник) другий фотон через квантовий канал («пінг»). Суб'єкт *A* випадковим чином перемикається між режимом передавання повідомлення й режимом контролю підслуховування.

У режимі передавання повідомлення суб'єкт *A* виконує унітарну операцію над отриманим від суб'єкта *B* фотоном для кодування інформації, а потім посилає його назад суб'єктові *B* («понг»). Чотири кодувальні операції суб'єкта *A* перетворюють стан $\left|\psi^+\right\rangle$ в стани $\left|\psi^+\right\rangle$, $\left|\psi^-\right\rangle$, $\left|\phi^+\right\rangle$ та $\left|\phi^-\right\rangle$ [13]. Ці стани й відповідають парам класичних біт «00», «01», «10» та «11». Коли суб'єкт *B* одержує фотон від суб'єкта *A*, він виконує вимірювання над обома фотонами в базисі Белла (2), щоб декодувати послану суб'єктом *A* двох-бітову комбінацію.

Крім режиму передавання повідомлення в пінг-понг протоколі передбачено також спеціальний режим контролю підслуховування, який призначений для виявлення атаки пасивного перехоплення [11, 13].

Як показано в багатьох роботах, наприклад [7, 9, 11, 13, 14], всі варіанти пінг-понг протоколу забезпечують тільки "асимптотичну" стійкість до атаки пасивного перехоплення, тобто атака буде виявлена з високою ймовірністю, але для цього потрібна деяка кількість режимів контролю підслуховування. Оскільки режими передавання повідомлення та контролю підслуховування чергуються випадковим чином, то до виявлення атаки зловмисник зможе одержати деяку кількість інформації. Як відзначено вище, такий витік інформації до зловмисника є неприпустимим для квантових протоколів прямого безпечного зв'язку.

Отже, виникає проблема підсилення стійкості пінг-понг протоколів, тобто створення таких методів попередньої обробки передаваної інформації, які зроблять перехоплену зловмисником інформацію некорисною для нього. Відповідний метод було розроблено в [19, 20], він полягає в наступному.

Перед передачею суб'єкт *A* розбиває своє двійкове повідомлення на *l* блоків деякої фіксованої довжини *r*, позначимо ці блоки через a_i ($i = 1,\ldots l$), а потім генерує для кожного блоку окремо випадкову оборотну двійкову матрицю K_i розміру $r \times r$ і множить отримані матриці на відповідні блоки повідомлення: $b_i = K_i a_i$. Отримані в результаті блоки

b_i передаються квантовим каналом з використанням пінг-понг протоколу.

Матриці K_i передаються суб'єктові B звичайним відкритим каналом після завершення квантової передачі, але тільки в тому випадку, якщо легітимні користувачі переконалися у відсутності підслуховування. Потім суб'єкт B обертає отримані матриці та, помноживши їх на відповідні блоки b_i, одержує початкове повідомлення. Розмір блоку r і відповідний розмір матриць K_i вибирається у залежності від потрібного рівня стійкості, тобто від потрібної ймовірності виявлення атаки [19–21]. Відзначимо, що описана процедура не є шифруванням повідомлення, а може бути названа "оборотним хешуванням".

У всіх реальних каналах зв'язку існують природні завади. Так як в протоколах квантової криптографії інформація передається окремими фотонами, то рівень завад при такому передаванні на багато порядків перевищує рівень завад у звичайних оптоволоконних лінях зв'язку та складає, як правило, порядку 10% і вище на відстанях в декілька десятків км. В протоколах квантового розподілення ключів, як відзначалось вище, для виправлення помилок використовують діалогові ітеративні процедури, наприклад каскадний протокол [3, 15]. Для протоколів прямого безпечного зв'язку, зокрема пінг-понг протоколів, такі процедури є неприйнятними, оскільки при їх виконанні відбувається витік інформації до зловмисника. В протоколах квантового розподілення ключів цей витік нівелюється на наступному етапі стеку протоколів – етапі підсилення секретності, де одержаний легітимними користувачами узгоджений бітовий рядок скорочується та перемішується. Зрозуміло, що така процедура не підходить для протоколів прямого безпечного зв'язку, а отже не підходять й діалогові процедури виправлення помилок. У даному випадку необхідно використовувати завадостійкі коди – кодування інформації, що передається, на передавальній стороні та відповідно її декодування на приймальній стороні.

На даний час розроблено низку квантових завадостійких кодів [1, 22], але вони призначені для виправлення самих квантових станів (тобто відновлення квантової інформації) і мають велику надлишковість. З іншого боку, пінг-понг протоколи (як і інші протоколи прямого безпечного зв'язку) призначені для передавання класичної інформації за допомогою квантового кодування. Тому для пінг-понг протоколів можна використовувати класичні завадостійкі коди, які виправляють пакети помилок, оскільки інформація в пінг-понг протоколах передається пакетами, починаючи з двох бітів для протоколу з переплутаними парами кубітів і квантовим надщільним кодуванням, який було розглянуто вище.

Зрозуміло також, що перед виконанням підсилення стійкості, тобто перед хешуванням повідомлення, його необхідно стиснути, наприклад, ентропійними методами стиснення.

На рис. 2 показано стек протоколів квантового прямого безпечного зв'язку з використанням пінг-понг протоколу у якості базового. Відзначимо, що на рис. 2 показано стек протоколів тільки для режиму передавання повідомлення. Контроль підслуховування в пінг-понг протоколі є окремим протоколом, і цей протокол також є частиною повного стека протоколів квантового прямого безпечного зв'язку [7, 13].

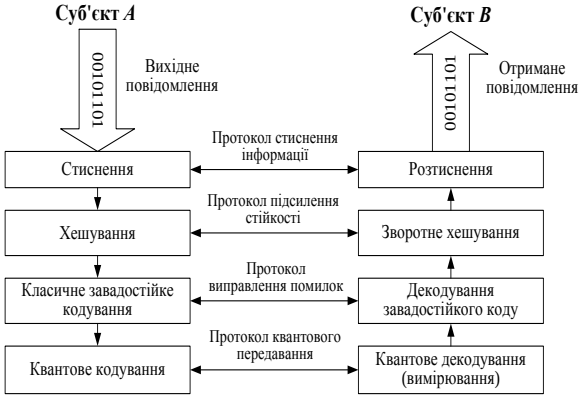

Рис. 2. Стек протоколів квантового прямого безпечного зв'язку

Висновки. В роботі детально проаналізовано стек протоколів квантового розподілення ключів, який ґрунтується на протоколі з передаванням одиночних кубітів – протоколі BB84. На підґрунті цього аналізу розроблено повний стек протоколів квантового прямого безпечного зв'язку на основі пінг-понг протоколу з переплутаними парами кубітів. Цей стек складається з наступних елементів: стиснення повідомлення; хешування блоків повідомлення для підсилення стійкості; завадостійке кодування хешованих блоків класичними кодами; передавання одержаних блоків інформації за допомогою пінг-понг протоколу. Розглянуто основні відмінності між стеками протоколів квантового розподілення ключів та квантового прямого безпечного зв'язку, які обумовлені різним призначення цих протоколів, різними типами передаваної інформації та відповідно різними вимогами до безпеки.

Розроблений стек протоколів квантового безпечного зв'язку придатний не тільки при використанні розглянутого в статті пінг-понг протоколу з переплутаними парами кубітів, а і при використанні будь-якого варіанту пінг-понг протоколу. Відповідні зміни стеку будуть стосуватися тільки протоколу хешування, де потрібно буде вибрати необхідний розмір матриць [14], а також відповідного методу завадостійкого кодування. Так, наприклад, для пінг-понг протоколу з n-кубітними станами Грінбергера–Хорна–Цайлінгера [21] буде потрібний завадостійкий код, що виправляє пакети помилок довжиною n бітів. В якості такого коду, як показують проведені раніше дослідження [23], може бути використаний код Файра.

Література

[1] Физика квантовой информации: Квантовая криптография. Квантовая телепортация. Квантовые вычисления / С.П. Кулик, Е.А. Шапиро (пер. с англ.); С.П. Кулик, Т.А. Шмаонов (ред. пер.); Д. Боумейстер и др. (ред.). — М.: Постмаркет, 2002. — С. 33–73.

[2] Gisin N. Quantum cryptography / N. Gisin, G. Ribordy, W. Tittel, H. Zbinden // Review of Modern Physics. — 2002. — V. 74, issue 1. — P. 145-195.

[3] Applied Quantum Cryptography / Kollmitzer C., Pivk M. (eds). — Springer-Verlag, Berlin, Heidelberg, 2010. — 227 p.

[4] Korchenko O. Quantum Secure Telecommunication Systems / Korchenko O., Vorobiyenko P., Lutskiy M., Vasiliu Ye., Gnatyuk S. // Telecommunications Networks — Current Status and Future Trends (Edited by J.H. Ortiz). — InTech, 2010. — P. 211-236.

[5] QPN Security Gateway (QPN–8505) // [Електронний ресурс]. — Режим доступу: http://www.magiqtech.com/MagiQ/Products.html

[6] QKS. Toshiba Research Europe Ltd., Cambridge Research Laboratory // [Електронний ресурс]. — Режим доступу: http://www.toshiba-europe.com/research/crl/qig/quantumkeyserver.html

[7] Bostrom K. Deterministic secure direct communication using entanglement / K. Bostrom, T. Felbinger // Physical Review Letters. — 2002. — V. 89, issue 18. — 187902.

[8] Ostermeyer M. On the implementation of a deterministic secure coding protocol using polarization entangled photons / M. Ostermeyer, N. Walenta // Optics Communications. — 2008. — V. 281, issue 17. — P. 4540-4544.

[9] Vasiliu E.V. Non-coherent attack on the ping-pong protocol with completely entangled pairs of qutrits / E.V. Vasiliu // Quantum Information Processing. — 2011. — V. 10, № 2. — P. 189–202.

[10] Wang C. Multi-step quantum secure direct communication using multi-particle Greenberger–Horne – Zeilinger state / C. Wang, F.G. Deng, G.L. Long // Optics Communications. — 2005. — V. 253, issue 1. — P. 15–20.

[11] Deng F.G. Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block / F.G. Deng, G.L. Long, X.S. Liu / Physical Review A. — 2003. — V. 68, issue 4. — 042317.

[12] Lin S. Quantum secure direct communication with chi-type entangled states / S. Lin, Q.Y. Wen, F. Gao, F.C. Zhu // Physical Review A. — 2008. — V. 78, issue 6. — 064304.

[13] Василиу Е.В. Анализ безопасности пинг-понг протокола с квантовым плотным кодированием / Е.В. Василиу // Наукові праці ОНАЗ ім. О.С. Попова.– 2007.– № 1.– С. 32–38.

[14] Василіу Є.В. Синтез структури квантових систем прямого безпечного зв'язку / Є.В. Василіу // Цифрові технології. — 2011, № 9. — С. 20-30.

[15] Василиу Е.В. Сравнительный анализ стойкости двух квантовых протоколов распределения ключей с передачей кубитов / Е.В. Василиу, С.М. Горохов // Наукові праці ОНАЗ ім. О.С. Попова. — 2006, № 2. — С. 70-77.

[16] Brassard G. Secret-key reconciliation by public discussion / G. Brassard, L. Salvail // Advanced in Cryptology: Proceedings of EUROCRYPT93, Lecture Notes in Comput. Sci. — 1994. — V. 765. — P. 410–423.

[17] Buttler W.T. Fast, efficient error reconciliation for quantum cryptography / W.T. Buttler, S.K. Lamoreaux, J.R. Torgerson et al // Physical Review A. — 2003. — V. 67, issue 5. — 052303.

[18] Elkouss D. Information Reconciliation for Quantum Key Distribution / D. Elkouss, J. Martinez-Mateo, V. Martin // Quantum Information Computing. — 2011. — V. 11. — P. 226-238.

[19] Василиу Е.В. Синтез основанной на пинг – понг протоколе квантовой связи безопасной системы прямой передачи сообщений / Е.В. Василиу, С.В. Николаенко // Наукові праці ОНАЗ ім. О.С. Попова. — 2009, № 1. — С. 83-91.

[20] Воробієнко П.П. Спосіб підсилення безпеки пінг-понг протоколу квантового безпечного зв'язку / П.П. Воробієнко, Є.В. Василіу, С.В. Ніколаєнко // Патент на корисну модель № 59732. - Дата реєстрації 25.05.2011.

[21] Василіу Є.В. Оцінки обчислювальної складності способу підсилення безпеки пінг–понг протоколу з переплутаними станами кубітів та кутритів / Є.В. Василіу, Р.С. Мамедов // Наукові праці ОНАЗ ім. О.С. Попова. — 2009, № 2. — С. 14-25.

[22] Прескилл Дж. Квантовая информация и квантовые вычисления / Прескилл Дж. — Т.1. — Ижевск: «Регулярная и хаотическая динамика», 2008. — 464 с.

[23] Николаенко С.В. Оценка корректирующей способности помехоустойчивого кода Файра для реализации пинг-понг протокола с парами перепутанных кубитов в квантовом канале с помехами / С.В. Николаенко, Е.В. Василиу // Захист інформації. — 2012, № 3(56). — С. 28-36.

УДК 004.056.53+530.145 (045)

Василиу Е.В. Стеки протоколов квантовой криптографии

Аннотация. *В статье детально проанализирован стек протоколов квантового распределения ключей, основанный на протоколе с передачей одиночных кубитов – протоколе BB84. На основе этого анализа разработан полный стек протоколов квантовой прямой безопасной связи на основе пинг-понг протоколов. Разработанный стек включает в себя такие основные протоколы: усиление секретности, помехоустойчивое кодирование, квантовая передача информации. При этом разработанный стек протоколов квантовой безопасной связи пригоден при использовании любого варианта пинг-понг протокола в качестве базового. Рассмотрены основные отличия между стеками протоколов квантового распределения ключей и квантовой прямой безопасной связи, которые обусловлены разным назначением этих протоколов, разными типами передаваемой информации и соответственно разными требованиями к их безопасности.*

Ключевые слова: *квантовая криптография, кубит, квантовые протоколы распределения ключей, квантовые протоколы прямой безопасной связи, стеки протоколов.*

Vasiliu Ye. Stacks of quantum cryptography protocols

Abstract. *In the paper the stack of protocols of quantum key distribution, based on the protocol with single qubits transmission (BB84 protocol), is in details analysed. Based on this analysis the full protocols stack of quantum secure direct communication on a basis of the ping-pong protocol is developed. The developed stack includes such basic protocols: privacy amplification, error correction coding, and quantum information transfer. At the same time developed stack of protocols of quantum secure communication is suitable at use of any variant of the ping-pong protocol as the base. The basic differences between stacks of protocols of quantum key distribution and quantum secure direct communication, which are caused by different purpose of these protocols, different types of the transferred information and accordingly different requirements to their security are considered.*

Key words*: quantum cryptography, qubit, quantum key distribution protocols, quantum secure direct communication protocols, stacks of protocols.*

Отримано *28 січня 2014 року*, затверджено редколегією *24 лютого 2014 року*